Journal of Technology Management and Business

IMPACT OF SCENARIO BASED EXERCISE ON ORGANISATION RESILIENCE IN CRITICAL INFRASTRUCTURE ORGANISATIONS

Arniyati Ahmad[1], Christopher William Johnson[2], Tim Storer[3]
[1]Department of Computer Science, National Defence University of Malaysia
[2,3]Department of Computing Science, University of Glasgow
Corresponding Email: arniyati@gmail.com

Abstract

Critical infrastructures are organisations that deliver vital services like telecommunication, energy and water suppliers to the community. Today, threats on critical infrastructure are differs from natural disasters, technical failures, man-made and cyber-attacks. Any disruptions on critical infrastructures could create a catastrophic damage. Protecting critical infrastructures and cultivating resilience has become a main agenda in many countries. Collaboration effort between public and private in crisis management through Scenario Based Exercise (SBE) was part of the agenda. SBE also known as Scenario Based Training (SBT) is a management tool used to train decision makers in crisis situations. However crisis management exercises through SBE appear to produce indistinct learning results which very limited in applicability. Using benchmark tool developed by Resilient Organisations Research at the University of Canterbury in New Zealand, this paper attempt investigate how SBE reflects the organisation resilience and determine the correlations between SBE and organisation resilience in critical infrastructures organisations.

Keywords: *Critical Infrastructure, Organisation Resilience, Scenario Based Exercise, Scenario Based Training, Scenario Based Planning.*

1.0 Introduction

National critical infrastructures provide services to the community like water supply, electricity, transportation, networks and communications (Boin and McConnell, 2007). These infrastructures are supported by information systems and connected through networks providing and exchanging information to support their critical services (Rinaldi, 2004; Boin and McConnell, 2007; Setola, Porcellinis and Sforna, 2009). Any disruption on these infrastructures will affect the social, economy and stability of the whole nation organisations (Boin and McConnell, 2007; Stewart, Kolluru & Smith, 2009; Alfred and Mike, 2010). Threats on critical infrastructures fall under several categories from natural disasters, man-made, technical error and cyber-attacks. Major critical infrastructures are owned by private organisations (Boin and McConnell, 2007; Borell and Eriksson, 2013). The collaboration between public and private become main agenda of National Critical Infrastructure Protection. One agenda of the collaboration efforts is through worst-case scenario exercise (Boin and McConnell, 2007; Borell and Eriksson, 2013). Scenarios has been used as a learning tool to explore general areas of risk and opportunity, this use normally leads to the development of more focused scenarios before decisions were made (Moats, Chermack and Dooley, 2008). The use of simulation exercises are often based on secretly developed scenarios and submitted within a compressed time frame to an unprepared crisis management team (Robert and Lajtha, 2002). Since of the chosen scenario is not considered to be particularly relevant by

the participants, this result in inadequate transfer of learning and less applicability to the organisation involved in the collaboration exercise (Robert and Lajtha, 2002).

This study is to investigate how SBE reflects the organisation resilience and to see any correlation between SBE and organisation resilience in critical infrastructures sectors. This paper was organised in 5 sections: Section 2 discuss the literature review on critical infrastructures SBE, Organisation Resilience and Resilience Benchmark Tool as the scope and focus of the paper. Section 3 provides the methodology used to collect data using the Organisation Resilience Benchmark Tool. Analysis and results was discussed in Section 4. Finally, findings and future works are summarised in Section 5.

2.0 Literature Review

Definitions of critical infrastructure are differs between countries (Choo, 2010). In the UK, a Centre for the Protection of National Infrastructure (CPNI) defined its Critical National Infrastructure (CNI) as "certain 'critical' elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life" (UK Cabinet office, Cyber Security Strategy, 2011). This categorization of CNI includes communications, emergency services, energy, finance, food, government and public services, health, transport and water (UK Cabinet office, Cyber Security Strategy, 2011). Threats to these critical infrastructures are grouped into two categories: physical threats to tangible property ("physical threats") and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats") (Boin and McConnell, 2007). Because of major critical infrastructures are owned by private organisations (Boin and McConnell, 2007; Stewart, Kolluru & Smith, 2009; Alfred and Mike, 2010). The collaboration efforts between public and private has become part of agenda in Critical Infrastructure Protection (Stewart, Kolluru & Smith, 2009) and one of the agenda is to collaborate in crisis exercise through SBE or SBT (Wybo, 2008; Solansky and Beck, 2009; Stewart, Kolluru & Smith, 2009).

Scenario Planning (SP), SBT and SBE are defined as two cutting-edge methods for organizational leaders to understand their environments to avoid devastating events and to put in place efficient and effective plans for surviving when the disasters strike (Peterson, Cumming, and Carpenter, 2003; Moats, Chermack and Dooley, 2008). The rationale of crisis management through SBE is to produce the transfer of useful learning results of future and unexpected crisis situations to their organisations (Borell and Eriksson, 2013; Woltjer, Trnka, Lundberg and Johansson, 2006). In contrast, SBE was found inadequate because of the chosen scenario is not considered to be particularly relevant by the participants (Robert and Lajtha, 2002). Another barrier to cross-agency collaboration include differences in organisational goals, professional cultures, line of accountability, political control styles and decision making cycles (Boin and McConnell, 2007). Nevertheless, in order to be prepared of any ambiguous crises and especially catastrophes, efforts should be focused on the promotion of resilience in critical infrastructure organisations (Boin and McConnell, 2007; Stewart, Kolluru & Smith, 2009; Alfred and Mike, 2010; Cornish, Livingstone, Clemente and Yorke, 2011).

Concept of resilience defined as the ability of an element or system to return to a stable safer after a disruption (Burnard and Bhamra, 2011). While there is an increasing acceptance of the concept within academic publications, the concept and features of organisational resilience are still largely undefined and ambiguous (Burnard and Bhamra, 2011; Burnard, Bhamra and Young; 2012). There are still ongoing

debates on concept of resilience, the improvements and expansions of the term (Burnard and Bhamra, 2011). In 2008, McManus defined organisation resilience as organisation function towards situational awareness, management of keystone vulnerabilities, and adaptive capacity involved in a complex, dynamic and interconnected environment. To enhance the organisation resilience concept developed by McManus (2008), Stephenson (2010) provided a benchmark tool for measuring organisation resilience. Using this tool organisation can review their scores for each of the indicators of organisational resilience and address their weaknesses and plan how to leverage off of their strengths in a crisis (Stephenson, 2010). Table 1 show 3 factors: Situation Awareness (SA), Management of Keystone Vulnerabilities (KV) and Adaptive Capacity with 21 indicators developed by Resilient Organisations Research at the University of Canterbury in New Zealand (McManus, 2008; Stephenson, 2010; Lee, Vargo and Seville, 2013) which will be used to assess the organisation resilience in this study.

Table 1: Organisation Resilience Indicators (Stephenson, 2010)

Situation Awareness	Management of Keystone Vulnerabilities	Adaptive Capacity
Roles & Responsibilities	Planning Strategies	Silo Mentality
Understanding & Analysis of Hazards & Consequences	Participation in Exercises	Communications & Relationships
Connectivity Awareness	Capability & Capacity of Internal Resources	Strategic Vision & Outcome Expectancy
Insurance Awareness	Capability & Capacity of External Resources	Information & Knowledge
Recovery Priorities	Organisational Connectivity	Leadership, Management & Governance Structures
Internal & External Situation Monitoring and Reporting	Robust Process for Identifying and Analysing Vulnerabilities	Innovation & Creativity
Informed Decision Making	Staff Engagement & Involvement	Devolved and Responsive Decision Making

3.0 Research Methodology

In order to determine the correlation between SBE and organisation resilience a preliminary study was conducted using Quantitative methods. The survey used a benchmark tool developed by Resilient Organisations Research at the University of Canterbury in New Zealand (McManus, 2008; Stephenson, 2010). This tool use 5-Likert Scale ranging from “Strongly Agree” to “Strongly Disagree”. The online

survey developed using Qualtrics software and published online has total number of 82 questions divided by three sections which cover background information (10 questions), Leadership and Culture (24 questions), Network (17 Questions) and Change Ready (31 Questions). The survey has been published for two months from September to November 2013.

The aim of the study is to see correlations between SBE and organisation resilience through following: Hypotheses:
H1: There is a relationship between SBE Experience and Organisation Resilience (OR)
H2: There is a relationship between SBE Experience and Adaptive Capacity (AC)
H3: There is a relationship between SBE Experience and Management of Keystone Vulnerabilities (KV)
H4: There is a relationship between SBE Experience and Situation Awareness (SA)

4.0 Data Analysis And Result

4.1 Demographic Analysis

In total there were 102 respondents from 10 sectors including: Electric/Power, Water Supplier, Nuclear, Telecommunication, Food Supplier, Internet Service Provider, Transport, Oil and Gas, Banking and Finance, and Government Service. The distribution of respondents from 11 critical infrastructures sectors as describe in Table 2 are; Electric/Power (4%),Water Supplier (1%), Nuclear (1%), Telecommunication (8%), Internet Service Provider (4%), Transport(1%), Oil and Gas (13%), Banking and Finance (3%), Government Service (55%), Health (6%) and Other (5%) but none from Food Supplier.

Table 2: Distribution of Respondents by Sector

Organization Sectors	Frequency	Percent
Electric/Power	4	3.9
Water Supplier	1	1.0
Nuclear	1	1.0
Telecommunication	8	7.8
Internet Service Provider	4	3.9
Transport	1	1.0
Oil and Gas	13	12.7

Banking and Finance	3	2.9
Government Service	56	54.9
Health	6	5.9
Other	5	4.9
Total	102	100.0

To study the correlation between Organisation Resilience (OR) and SBE, the data has been grouped into two groups of participants that have SBE experience and without SBE experience. Table 3 shows the distribution of the 39 participants with SBE experience and 61 participants without SBE experience. A reliability test was conducted using Cronbach's α to see internal consistency of the benchmarks tool items (Stephenson, 2010). The reliability test result was used to calculate the Organisation Resilience (OR) using Relative Overall Resilience (ROR) equation in Stephenson (2010), then correlation test was then conducted between OR and SBE groups. Section 4 provides details discussion on the results and analysis of the study.

Table 3: Distribution of Respondents with SBE Experience

SBE Experience	Frequency	Percent
Yes	39	38.2
No	63	61.8
Total	102	100.0

4.2 Reliability Analysis

Reliability test was conducted on organisation resilience indicators to measure the internal consistency of the benchmark tool used (Lee, Vargo and Seville, 2013). Cronbach's Alpha coefficient commonly used as indicator of internal consistency should have values 0.7 or above to indicate strong item covariance (Pallant, 2010). Table 4 shows the Cronbach's Alpha coefficient for the organisation resilience indicators ranged from 0.709 to 0.837. Items that have Cronbach's Alpha coefficient below 0.7 have been removed and the reliability test result was then used to calculate the Organisation Resilience (OR) score using Relative Overall Resilience (ROR) equation in Stephenson (2010). As outlier has an effect on correlation coefficient (Pallant, 2010), boxplot graph has been used to identify the outliers and some outlier has been removed from the dataset.

Table 4: Reliability of OR Indicators

Dimension/ Factor	Indicator	Cronbach's α	Cronbach's α based on standardised items	No of items
AC	Information & Knowledge	0.729	0.727	3
	Leadership, Management & Governance Structures	0.724	0.716	5
	Innovation & Creativity	0.729	0.738	3
	Devolved & Responsive Decision Making	0.784	0.788	3
KV	Participation in Exercises	0.804	0.804	2
	Capability & Capacity of Internal Resources	0.837	0.840	2
	Capability & Capacity of External Resources	0.745	0.749	2
	Organisational Connectivity	0.824	0.829	2
SA	Role & Responsibilities	0.707	0.713	3
	Connectivity Awareness	0.709	0.709	2
	Recovery Priorities	0.796	0.799	3
	Internal & External Situation Monitoring & Reporting	0.734	0.733	3

4.3 Correlation Analysis

Pearson's correlation is a measure of strength of the association of two or more variables (Pallant, 2010). The strength of the relationship between two variables was determined by correlation coefficient and the significance (Pallant, 2010). The correlation coefficient normally used as Pearson's *r* show the strong positive or negative relationship between -1 to +1 (Pallant, 2010). It also provides direction of

relationship between two variables. While the significance (Sig), shows confidence on the obtained results. This study used to see any relationship of SBE Experience with organisation resilience.

1) Correlation between SBE Experience with organisation resilience

Table 5: Correlation between SBE and Organisation Resilience

SSBE Experience	Organisation Resilience (OR)
Pearson Correlation	0.112
Sig. (2-tailed)	0.271
N	99

** Correlation is significant at the 0.05 level (2-tailed)*

Table 5 shows the results of a Pearson's correlation *r* value of 0.112 which indicate weak relationship (1%) between SBE Experience and Organisations Resilience (OR). This relationship is also not significant with Sig=0.271 which fall outside 0.05, this reject the hypothesis which indicates that there is no relationship between SBE Experience and organisation resilience.

2) Correlation between SBE Experience with organisation resilience factors

This correlation test is to see any relationships between SBE Experience and organisation resilience factors including: Adaptive Capacity (AC), Management of Keystone Vulnerabilities (KV) and Situation Awareness (SA). Table 6 and Table 7 show the results of a Pearson's correlation *r* value of 0.03 for AC and *r* value of 0.100 for KV, which both results indicate weak relationship between SBE Experience and Adaptive Capacity (AC), also weak relationship between SBE Experience and Keystone Vulnerabilities (KV). Both relationships results also not significant with value of Sig=0.977 for AC and Sig=0.325 for KV, which reject the H2 and H3, so there are no relationship between SBE Experience with Adaptive Capacity and also no relationship between SBE Experience with Keystone Vulnerabilities.

Table 6: Correlation between SBE and Adaptive Capacity

SSBE Experience	Adaptive Capacity (AC)
Pearson Correlation	0.003
Sig. (2-tailed)	0.977
N	99

Table 7: Correlation between SBE and Management of Keystone Vulnerabilities

SSBE Experience	Management of Keystone Vulnerabilities (KV)
Pearson Correlation	0.100
Sig. (2-tailed)	0.325
N	99

Table 8 shows the results of a Pearson's correlation r value of 0.209 (4%) for Situation Awareness (SA). Even though it shows a weak relationship between SBE Experience and Situation Awareness (SA), this result is significant with Sig=0.038 within 0.05, so H4 is accepted. This indicates a relationship between SBE Experience and Situation Awareness, but further investigation need to be done to confirm the result.

Table 8: Correlation between SBE and Situation Awareness

SSBE Experience	Situation Awareness (SA)
Pearson Correlation	0.209*
Sig. (2-tailed)	0.038
N	99

** Correlation is significant at the 0.05 level (2-tailed)*

3) Correlation between SBE Experience with organisation resilience indicators

Table 9 shows the correlation test on organisation resilience indicators from reliability test results as in Table 4. From 12 organisation resilience indicators used, it shows only 3 indicators that have relationship with SBE Experience. Though it shows weak relationships with Pearson's correlation r value of 0.220 (5%) for Capability and Capacity of External Resources, Pearson's correlation r value of 0.250 (6%) for Connectivity Awareness, Pearson's correlation r value of 0.201 (4%) for Recovery Priorities. In addition, there also showed a negative relationship between SBE and Devolved & Responsive Decision Making with *r=-0.197*, and a negative relationship between SBE and Capability & Capacity of Internal Resources *with r=-0.116.* Further investigation need to be done on these findings, as it not supported idea of SBE as

Table 9: Correlation between SBE and OR Indicators

Dimension /Factor	Organisation Resilience Indicator	SBE Experience	(n=99)
AC	Information & Knowledge	Pearson Correlation	.089
		Sig. (2-tailed)	.382
	Leadership, Management & Governance Structures	Pearson Correlation	.153
		Sig. (2-tailed)	.132
	Innovation & Creativity	Pearson Correlation	.028
		Sig. (2-tailed)	.782
	Devolved & Responsive Decision Making	Pearson Correlation	-.197
		Sig. (2-tailed)	.051
KV	Participation in Exercises	Pearson Correlation	.147
		Sig. (2-tailed)	.148
	Capability & Capacity of Internal Resources	Pearson Correlation	-.116
		Sig. (2-tailed)	.255
	Capability & Capacity of External Resources	Pearson Correlation	.220*
		Sig. (2-tailed)	.029
	Organisational Connectivity	Pearson Correlation	.044
		Sig. (2-tailed)	.669

SA	Role & Responsibilities	Pearson Correlation	.140
		Sig. (2-tailed)	.167
	Connectivity Awareness	Pearson Correlation	.250*
		Sig. (2-tailed)	.013
	Recovery Priorities	Pearson Correlation	.201*
		Sig. (2-tailed)	.046
	Internal & External Situation Monitoring & Reporting	Pearson Correlation	.088
		Sig. (2-tailed)	.386

** Correlation is significant at the 0.05 level (2-tailed)*

5.0 Conclusion And Future Works

As conclusion, this study is to investigate the relationship between Scenarios based Exercise (SBE) and Organisation Resilience (OR), through the correlation test results; it indicates that there is not enough evidence to see the relationship between Scenarios based Exercise and Organisation Resilience. While the investigation on relationships between SBE Experience and organisation resilience's factors show a weak relationship between SBE Experience and Situation Awareness (SA). This result supports a theory that SBE contributes to the situation awareness especially when involved command controls systems (Woltjer, Trnka, Lundberg and Johansson, 2006). Although adaptive capacity and management of keystone vulnerabilities are important elements that contributes to organisation's resilience in coping with disasters (Woltjer, Trnka, Lundberg and Johansson, 2006; Burnard and Bhamra, 2011; Burnard, Bhamra and Young; 2012), there were lack evidence to support relationship between SBE Experience with both factors. Another correlation results show relationships between SBE Experience with organisation resilience indicators of Capability and Capacity of External Resources, Connectivity Awareness and Recovery Priorities. Even though the results of this study have not provided strong enough evidences to relate the relationship of SBE with organisation resilience, further research was suggested to use the organisation resilience benchmark tool to assess the effectiveness of SBE in pre and post SBE environment. Since there were no available literature in how to assess the effectiveness of SBE in cultivating resilience this idea should be part of the future research in investigation resilience in critical infrastructures collaboration exercises.

6.0 Acknowledgement

Benchmark organisation resilience questions are copyright to Resilient Organisations Research at the University of Canterbury in New Zealand. The survey questions were used with permission.

7.0 References

Alfred.R.B and Mike W., 2010. ," A Framework for. Establishing Critical. Infrastructure Resilience. Goals". Final Report and Recommendations, National Infrastructure Advisory Council

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management, 15(1), 50-59.

Borell, J., & Eriksson, K. 2013. "Learning effectiveness of discussion-based crisis management exercises". International Journal of Disaster Risk Reduction

Burnard, K., & Bhamra, R. 2011. "Organisational resilience: development of a conceptual framework for organisational responses". International Journal of Production Research, 49(18), 5581-5599.

Burnard, K., Bhamra, R., & Young, R. I. 2012. Critical Factors of Organisational Resilience.

Centre for the Protection of National Infrastructure, 'Critical National Infrastructure', www.cpni.gov.uk/about/cni

Choo. K. K. R. 2010. High tech criminal threats to the national information infrastructure. information security technical report, 15(3), 104-111

Cornish. P., Livingstone, D., Clemente, D., & Yorke, C., 2011. Cyber Security and the UK's Critical National Infrastructure. A Chatham House Report. The Royal Institute of International Affairs.

Guthrie,P. and Konaris, T., 2012."Infrastructure Resilience", Commissioned Review, Foresight, Government Office for Science.

Lee, A. V., Vargo, J., & Seville, E. 2013. "Developing a Tool to Measure and Compare Organizations' Resilience". Natural Hazards Review, 14(1), 29-41.

McManus, S. T. 2008. Organisational resilience in New Zealand

Moats, J. B., Chermack, T. J., & Dooley, L. M. 2008. "Using scenarios to develop crisis managers: Applications of scenario planning and scenario-based training". Advances in Developing Human Resources, 10(3), 397-424

O'Rourke, T. D. 2007." Critical infrastructure, interdependencies, and resilience". Bridge-Washington-National Academy Of Engineering-, 37(1), 22.

Pallant, J. 2010. SPSS survival manual: A step by step guide to data analysis using SPSS. McGraw-Hill International.

Peterson, G. D., Cumming, G. S., & Carpenter, S. R. 2003. "Scenario planning: a tool for conservation in an uncertain world". Conservation biology, 17(2), 358-366.

Rinaldi, S. M. (2004, January). Modelling and simulating critical infrastructures and their interdependencies. In System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on (pp. 8-pp). IEEE

Robert, B., & Lajtha, C. 2002. "A new approach to crisis management. Journal of Contingencies and Crisis Management", 10(4), 181-191.

Setola, R., De Porcellinis, S., & Sforna, M. (2009). Critical infrastructure dependency assessment using the input–output inoperability model. International Journal of Critical Infrastructure Protection, 2(4), 170-178. Stephenson, A. V.2010. Benchmarking the resilience of organisations.

Stewart, G. T., Kolluru, R., & Smith, M. 2009. Leveraging public-private partnerships to improve community resilience in times of disaster. International Journal of Physical Distribution & Logistics Management, 39(5), 343-364.

The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. 2011. UK Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Woltjer, R., Trnka, J., Lundberg, J., & Johansson, B. 2006. Role-playing exercises to strengthen the resilience of command and control systems. In Proceedings of the 13th Eurpoean conference on Cognitive ergonomics: trust and control in complex socio-technical systems (pp. 71-78). ACM.

Wybo, J. L. 2008. "The role of simulation exercises in the assessment of robustness and resilience of private or public organizations". In Resilience of Cities to Terrorist and other Threats (pp. 491-507). Springer Netherlands.